Department for Digital, Culture, Media & Sport

We thank you for your time spent taking this survey.
Your response has been recorded.

Below is a summary of your responses

Download PDF

Digital identity and attributes consultation survey

This is the survey for the digital identity and attributes consultation. Please read the proposals before responding to this survey. A summary of questions asked in this survey can be found at the bottom of the document.

The online survey allows you to save a draft response and return to the survey later. You do not have to answer every consultation question and there is a confirmation page before a response is submitted.

Using the online survey greatly assists in our analysis of the responses, enabling more efficient and effective consideration of the issues raised for each question.

The consultation and online survey will last for eight weeks, opening 19 July and closing at 11:59 PM 13 September.

For enquiries about responding to the survey, please contact digital-identity-consultation@dcms.gov.uk. The privacy notice associated with this email can be found here.

Privacy notice:

Who is collecting my data?

The Department for Digital, Culture, Media & Sport (DCMS) helps to drive growth, enrich lives and promote Britain abroad.

We protect and promote our cultural and artistic heritage and help businesses and communities to grow by investing in innovation and highlighting Britain as a fantastic place to visit. We help to give the UK a unique advantage on the global stage, striving for economic success.

Purpose of this Privacy Notice

This notice is provided within the context of the changes required by the Article 13 & 14 of UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). This notice sets out how we will use your personal data as part of our legal obligations with regard to Data Protection. DCMS' personal information charter (opens in a new tab) explains how we deal with your information. It also explains how you can ask to view, change or remove your information from our records.

What is personal data?

Personal data is any information relating to an identified or identifiable natural living person, otherwise known as a 'data subject'. A data subject is someone who can be recognised, directly or indirectly, by information such as a name, an identification number, location data, an online identifier, or data relating to their physical, physiological, genetic, mental, economic, cultural, or social identity. These types of identifying information are known as 'personal data'. Data protection law applies to the processing of personal data, including its collection, use and storage.

What personal data do we collect?

Most of the personal information we collect and process is provided to us directly by you. This includes:

- Your name or the name of your organisation, your email address (if you decide to provide these details to us)
- Information on how you use this website. This includes IP address and analytical cookies

How will we use your data?

The personal data we process are the details of individuals who respond to the consultation – name, email address and phone number. This is processed by DCMS for the purposes of the consultation, so we can respond to your queries and views. It may also include using your personal data to invite you to events relating to the consultation. Finally, there may be a need to follow up in the aftermath of the consultation on the same topic or closely related topics.

What is the legal basis for processing my data?

The Data Protection Legislation states that, as government departments, the departments may process personal data as necessary for the effective performance of a task carried out in the public interest (i.e. a consultation). U.K. GDPR Art. 6 (1) e.

What will happen if I do not provide this data?

We will not be able to follow up with you regarding your survey response.

Who will your data be shared with?

Copies of responses may be published after the survey closes. If we do so, unless you indicate otherwise, we will ensure that neither you nor the organisation you represent are identifiable, and any responses used to illustrate findings will be anonymised.

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Departments.

How long will my data be held for?

Your personal data will be held for two years after the survey is closed. This is so that the department is able to contact you regarding the result of the

survey following analysis of the responses.

Will my data be used for automated decision making or profiling?

We will not normally use your data for any automated decision making. If we need to do so, we will let you know.

Will my data be transferred outside the UK and if it is how will it be protected?

We will not send your data overseas.

What are your data protection rights?

You have rights over your personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The Information Commissioner's Office (ICO) is the supervisory authority for data protection legislation, and maintains a full explanation of these rights on their website

DCMS will ensure that we uphold your rights when processing your personal data.

How do I complain?

You can find out more here: Personal information charter

The contact details for the data controller's Data Protection Officer (DPO) are:

Data Protection Officer

The Department for Digital, Culture, Media & Sport

100 Parliament Street

London

SW1A 2BQ

Email: dpo@dcms.gov.uk

If you're unhappy with the way we have handled your personal data and want to make a complaint, please write to the department's Data Protection Officer or the Data Protection Manager at the relevant agency. You can contact the department's Data Protection Officer using the details above.

How to contact the Information Commissioner's Office

If you believe that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. You may also contact them to seek independent advice about data protection, privacy and data sharing.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Website: www.ico.org.uk

Telephone: 0303 123 1113

Email: casework@ico.org.uk

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

Changes to our privacy notice

We may make changes to this privacy policy. In that case, the 'last updated' date at the bottom of this page will also change. Any changes to this privacy policy will apply to you and your data immediately.

If these changes affect how your personal data is processed, DCMS will take reasonable steps to let you know.

This notice was last updated on 19/07/2021.

Demographic questions

Are you filling in this survey as a private citizen or on behalf of an organisation?

- ○ Private citizen
- ● Organisation

Are you willing to be contacted regarding your response to this survey?

- ● Yes
- ○ No

Please provide your details:

Name:	Judith Crawford
Name of the organisation:	Electronic Money Association
Email address:	judith.crawford@e-ma.org

Would you like your response to remain confidential?

- ○ Yes
- ● No

Creating a digital identity governance framework

The governing body

1. Do you agree an existing regulator is best placed to house digital identity governance, or should a new body be created?

The EMA appreciates the arguments put forward in the Consultation (cost to the taxpayer, time to stand up a new regulator) in support of the assignment of the role of the Governing Body for the Framework to an existing regulator. However, we are concerned that no single UK regulator currently has the resources, expertise and experience to fulfil all the responsibilities that the Governing Body is expected to fulfil. For example, we do not believe any single UK regulator currently has access to the resources or expertise required to (i) Monitor the operational performance of the Digital ID framework or to (ii) generate requirements and standards to prevent fraud and cybercrime within the Framework (Clause 2.7.0.2 of the Consultation). We encourage DCMS to consider this point and seek to enable

the Governing Body to gain access to the required resource/expertise through collaboration with other UK regulators and through the establishment of Advisory/Working Groups. Academic and industry experts could be invited to join such groups to enable the Governing Body to benefit from national pools of digital ID framework expertise.

Characters remaining: 3852

2. Which regulator do you think should house digital identity governance?

As per the comments above, the EMA is not certain that any single UK regulator currently has the resources or expertise to fulfil all the responsibilities of the Governing Body listed in the Consultation. Our perception is that the required Governing Body expertise currently reside across a number of regulators (ICO, the FCA), government entities (NCSC) and private/industry groups (JMLSG, Financial Fraud Action etc.). It may be useful to consider assigning the role of Governing Body to a lead regulator that can then secure access to the necessary resource/expertise through co-operation agreements established with other parties referenced above.

Characters remaining: 4340

3. What is your opinion on the governance functions we have identified as being required: is anything missed or not needed, in your view?

The Governing Body responsibilities (listed in Clause 2.0.0.5) of the Consultation are appropriate.

Characters remaining: 4899

Creating a digital identity governance framework

Trust framework, standards and rules management

4. What is your opinion on the governing body owning the trust framework as outlined, and does the identity of the governing body affect your opinion?

Our perception is that is appropriate for the Governing Body to own the Trust Framework standards/requirements. We invite DCMS to clarify the statement that appears in Clause 2.2.1.3 of the Consultation that ".... updates to standards, requirements or associated guidance will not necessarily need to be made by the governing body itself. The governing body may arrange for the updates to be made by others, whilst remaining in overall oversight and ownership." It is our view that future Trust Framework updates should be carried out under the control of the Governing Body and involve academic and industry experts as well as representatives of participants in the UK Digital ID ecosystem and of other UK regylators as well as consumer/data subject groups.

Characters remaining: 4235

5. Is there any other guidance that you propose could be incorporated into the trust framework?

DCMS should consider expanding the Trust Framework to provide: - Implementation guidance to digital

ID ecosystem participants on specific topics (cybersecurity, digital ID fraud management) - More detail on notification requirements related to specific events (incidents, service availability status changes, lifecycle management events) for ecosystem participants.

Characters remaining: 4632

6. How do we fairly represent the interests of civil society and public and private sectors when refreshing trust framework requirements?

We encourage DCMS to consider the establishment of Advisory/Working Groups composed of representatives of relevant stakeholders (industry experts, academics, data subject group representatives, representatives of other UK regulators) that will work under the guidance of the Governing Body to update Trust Framework requirements in a structured, transparent fashion.

Characters remaining: 4633

7. Are there any other advisory groups that should be set up in addition to those suggested?

We encourage the Governing Body to consider establishing focused Advisory Groups to support the review of specific areas of the Trust Framework requirements in areas like Cybersecurity, Fraud Management, Interoperability and Inclusion.

Characters remaining: 4762

Creating a digital identity governance framework

Accreditation & certification

8. How should the government ensure that any fees do not become a barrier to entry for organisations while maintaining value for money for the taxpayer?

We encourage the government to ensure that access to UK Digital ID ecosystem is widely available. The access fees' structure should be informed by the (i) Size of applicant entities, (ii) Role of applicants, (iii) Scope and volume of access of Digital ID data/attributes datasets (for example, instances of access of the Legal Gateway).

Characters remaining: 4659

Creating a digital identity governance framework

Oversight/Management of organisations/schemes

9. Do you agree with this two-layered approach to oversight where oversight is provided by the governing body and scheme owners?

We believe it is important that the Governing Body: - Ensures that Scheme specifications are assessed

We believe it is important that the Governing Body: - Ensures that Scheme specifications are assessed for alignment with Trust Framework requirements on an ongoing basis, - Ensures that individual Scheme specifications do not impact cross-industry Framework interoperability and access, - Establishes an Escalation/Arbitration process that individual Scheme participants can use to liaise with the Governing Body to seek assistance in ongoing Trust Framework access disputes with individual Scheme owners, - Ensures that any future Scheme Accreditation (per Cl. 2.5.0.2) does not impact ongoing monitoring of Scheme activities.

Characters remaining: 4366

Creating a digital identity governance framework

Complaints, redress and enforcement

10. Do you agree the governing body should be an escalation point for complaints which cannot be resolved at organisational or scheme level?

We agree that the Governing Body should act as an escalation point for complaints/disputes involving ecosystem participants (including within Schemes) and/or consumers/data subjects. The benefits of the establishment of a Dispute Resolution mechanism/process could also be considered during the establishment of complaints management processes.

Characters remaining: 4651

11. Do you think there needs to be additional redress routes for consumers using products under the trust framework?

- (●) Yes
- ( ) No

If yes, which one or more of the following?

- [x] A governing body-led ombudsman service
- [ ] Industry-led dispute resolution mechanism (encouraged or mandated)
- [x] Set contract terms between organisations and consumers
- [ ] Something else
- [ ] Any further comment

12. Do you see any challenges to this approach of signposting to existing redress pathways?

It may prove a challenge to establish adequate redress pathways that increase consumer/data subject confidence while not raising barriers to joining the UK Digital ID ecosystem for private entities of varying sizes.

Characters remaining: 4784

13. How should we enhance the ‘right to rectification’ for trust framework products and services?

The Governing Body may consider establishing performance standards requirements for the execution of identify repairs after the submission of valid "right to rectification" requests. Adherence to such standards can form part of the certification and ongoing monitoring process for digital ID ecosystem participants that hold the relevant roles (Identity Service Provider, Attributes' Data Owner). Our view is that the responsibility for the completion of identity repairs should be assigned to the owner of the underlying dataset that holds inaccurate/corrupted digital identity data.

Characters remaining: 4410

14. Should the governing body be granted any of the following additional enforcement powers where there is non-compliance to trust framework requirements?

- [x] Monetary fines
- [x] Enforced compensation payments to affected consumers
- [x] Restricting processing and/or provision of digital identity services
- [x] Issue reprimand notices for minor offences with persistent reprimands requiring further investigation
- [ ] Any further comment

15. Should the governing body publish all enforcement action undertaken for transparency and consumer awareness?

Our view is that Governing Body should publish details of enforcement action it undertakes for the benefit of consumers and other UK digital ID ecosystem participants.

Characters remaining: 4832

Creating a digital identity governance framework

Security & Fraud

16. What framework-level fraud and security management initiatives should be put in place?

We encourage the Governing Body to consider the establishment of dedicated Cybersecurity and Fraud Management Working Groups that are tasked with tracking (i) cybersecurity threats and (ii) fraud typologies that impact digital ID ecosystem participants. These Working Groups can drive the generation and dissemination of actionable intelligence on Cybersecurity and Fraud Management to ecosystem participants. It is also advisable to consider establishing collaboration arrangements with UK government entities that operate well-established information services in the fields of cybersecurity

government entities that operate well-established information services in the fields of cybersecurity (NCSC) and fraud management (CIFAS, Financial Fraud Action UK etc.).

Characters remaining: 4332

Creating a digital identity governance framework

Inclusion

17. How else can we encourage more inclusive digital identities?

We encourage DCMS (and the Governing Body) to continue to track ease of access to digital ID framework assets/services by specific categories of users with limited access to existing physical ID solutions. The option to allow in-person digital ID creation will increase the scope of access to digital services enabled by the Trust Framework. Enabling the use of digital ID data/attributes to access physical services will increase the appeal of the ecosystem to individual consumers with more limited digital literacy.

Characters remaining: 4474

18. What are the advantages and disadvantages with this exclusion report approach?

An advantage of the proposed annual Exclusion Report generation/submission requirement is that it will increase the focus of identity service/solution providers on the scope of access to their service offered to different consumers. An unintended consequence may be that the costs associated with the requirement to generate the Report acts as a barrier to entry for small/medium size identity service providers. We encourage the Governing Body to ensure a consistent approach to addressing Inclusion gaps in the delivery of digital ID service gaps across different industries/Schemes.

Characters remaining: 4408

19. What would you expect the exclusion report to include?

The Exclusion Report topics that are listed in the Consultation (Clause 2.8.1.4) are appropriate. It may be useful to encourage ecosystem participants to provide an update on the implementation of remedial actions identified in earlier Reports.

Characters remaining: 4753

Enabling a legal gateway between public and private sector organisations for data checking

Protecting privacy and individuals

20. Should membership of the trust framework be a prerequisite for an organisation to make eligibility or identity checks against government-held data?

Our view is that parties seeking to carry out eligibility/identity checks of data subjects using the Legal Gateway must sign up to a limited set of requirements and/or a Code of Conduct. In this context, some level of ecosystem membership by these Relying Parties is likely appropriate.

Characters remaining: 4711

21. Should a requirement to allow an alternative pathway for those who fail a digital check be set out in legislation or by the governing body in standards?

The intention appears to be to ensure that service providers enable alternative services paths that do not involve a digital ID check. In this context, it would be appropriate to set out this requirement in separate legislation. We note that it may prove increasingly challenging to provide alternative access paths to digitally-native (or digital-only) services for consumers that fail digital ID checks.

Characters remaining: 4592

Enabling a legal gateway between public and private sector organisations for data checking

How data could be checked

22. Should disclosure be restricted to a “yes/no" answer or should we allow more detailed responses if appropriate?

The delivery of more detailed responses to attribute checks should be enabled to facilitate more complex attributes' checking use Cases. We encourage the Governing Body to adopt the use of Data Loss Prevention (DLP) principles in the design of data checking interfaces to minimise information leakage.

Characters remaining: 4694

23. Would a code of practice be helpful to ensure officials and organisations understand how to correctly check information?

The establishment of a Code of Practice (as part of the Trust Framework) that is adopted by all ecosystem participants will help increase consumer and organisation confidence in the ecosystem. The adherence of ecosystem participants to the Code of Practice should be monitored on an ongoing basis.

Characters remaining: 4698

24. What are the advantages or disadvantages of allowing the onward transfer of government-confirmed attributes, as set out?

We perceive the primary advantage of allowing onward transfer of government-confirmed attributes to be a more frictionless customer experience in accessing similar services within a short period of time. However, there are also disadvantages associated with affording this capability (potential information leakage to ineligible relying parties, data subject confusion and perception of lack of control, increased

leakage to ineligible relying parties, data subject confusion and perception of lack of control, increased complexity of identity repair impact assessments).

Characters remaining: 4531

Establishing the validity of digital identities and attributes

25. Would it be helpful to affirm in legislation that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents?

We believe that it will be useful to seek to confirm in national legislation the equivalence of digital identities/attributes with physical identification forms in the context of securing controlled access to services.

Characters remaining: 4780

Warning, pressing the proceed button will submit your response and you will not be able to submit another response through the survey.

If you do wish to change some of your answers after submitting, please contact digital-identity-consultation@dcms.gov.uk. The privacy notice associated with this email can be found here.

A copy of your responses will be provided to you after you press the proceed button.